Юридические исследования
Правильная ссылка на статью:
Алиев Т.Ф. — Вопросы противодействия преступлениям, совершаемым с использованием IT-технологий // Юридические исследования. – 2023. – № 10. DOI: 10.25136/2409-7136.2023.10.44173 EDN: BDIKBI URL: https://nbpublish.com/library_read_article.php?id=44173

Вопросы противодействия преступлениям, совершаемым с использованием IT-технологий

Алиев Тимур Фирудинович

ORCID: 0000-0002-0645-931X

младший лейтенант полиции, слушатель факультета правоохранительной деятельности, Восточно-Сибирский институт МВД России

664017, Россия, Иркутская область, г. Иркутск, ул. Лермонтова, 110

timuraliev.2018@mail.ru

Статья из рубрики "Юридический практикум"

DOI:

10.25136/2409-7136.2023.10.44173

EDN:

BDIKBI

Дата направления статьи в редакцию:

29-09-2023

Аннотация: Предметом настоящего исследования являются особенности противодействия преступлениям, совершаемым с использованием IT-технологий. Цель работы заключается в рассмотрении и разрешении отдельных проблемных аспектов вопроса о противодействии IT-преступлениям. Методология исследования основана на общенаучных и частно-научных методах познания — диалектическом, логическом, статистическом, сравнительно-правовом, формально-юридическом, правового прогнозирования. Актуальность выбранной тематики имеет как теоретический, так и практический аспекты значимости в современных реалиях. Так, в контексте информатизации общества важно защищать информационную безопасность от киберугроз. В современном мире информационные технологии используются, к сожалению, не только законопослушными гражданами, в связи с чем встает вопрос об обеспечении национальной кибербезопасности. На сегодняшний день данный вид преступлений носит межгосударственный характер в силу большого количества их совершения. Киберпреступность растет в масштабах, и это подтверждается следующими

статистическими данными: с 2014 по 2022 г. был зафиксирован практически пятидесятикратный рост IT-преступлений (10 тыс. против 510 тыс. киберпреступлений). Автор представленной статьи пришёл к выводу о том, что противодействие IT-преступлениям должно осуществляться с учётом научно-технического прогресса. Изучая международный опыт, анализируя современные отечественные способы противоборства данной категории преступности, автор убедился, что является важным использовать цифровые технологии в противодействии IT-преступлениям, применение которых поможет снизить как количество совершения данного рода преступных деяний, так и повысить процент раскрываемости данной категории преступности. Автором проиллюстрированы примеры того, как искусственный интеллект может служить «верным помощником» в отечественной практике противодействия IT-преступлениям. Помимо этого, приоритетным является совершенствование знаний и навыков сотрудников правоохранительных органов по противодействию данной категории преступности, в то же время необходимо проводить профилактические мероприятия с целью осведомленности населения об основных преступных схемах злоумышленников.

Ключевые слова:

киберпреступность, IT-технологии, противодействие, научно-технический прогресс, профилактика, совершенствование деятельности, искусственный интеллект, роль специалиста, динамичный характер, приоритетное направление

Цифровизация населения охватывает многие сферы жизнедеятельности, позволяя более эффективно решать те или иные задачи. Информационно-телекоммуникационные технологии (далее по тексту — ИТТ; IT-технологии) неразрывно связаны с научно-техническим прогрессом, и в век цифровых технологий проблематично представить человека, не пользующегося смартфоном, ноутбуком или иным гаджетом. Нет никаких сомнений в удобстве и практичности цифровых технологий, например, в решении бытовых вопросов с использованием мессенджеров или поисковых систем.

С другой стороны, прогрессирование IT-технологий, помимо своих неоспоримых преимуществ, имеет и обратную сторону: всё более распространенным становится совершение мошенничеств, вымогательств, хакерских взломов, незаконного оборота наркотических средств, распространения вирусных программ и проявления других противоправных действий с использованием информационных технологий [1, с. 221—224]. Небезызвестен факт: «состояние преступности является своеобразным отражением, индикатором процессов, происходящих в обществе» [2, с. 99].

Развитие информационных технологий, в частности, сказалось на новых способах совершения киберпреступлений. Так, компьютерная сеть превратилась в новый эффективный инструмент для ведения бизнеса и новый мощный канал распространения преступных деяний. В связи с этим, думается, необходимо прорабатывать наиболее оптимальные и эффективные формы их противодействия [3, с. 222; 4, с. 16]. Действительно, в век цифровых технологий проблема киберпреступности отличается острой злободневностью, и противодействие ей имеет как теоретическую, так и практическую значимость.

В настоящем исследовании автором использованы труды отечественных ученых А. А. Балашовой, А. А. Баранова, О. П. Грибунова, К. Н. Евдокимова, А. А. Остапенко, С. В Пархоменко, Н. А. Полторацкого, Ю. Л. Соловьёвой, С. В. Тимофеева, Е. И. Третьяковой,

С. И. Усачева и др., многие из которых являются признанными учеными в области противодействия киберпреступлениям. Труды приведенных исследователей, полагаем, соответствуют теме исследования, обладают признаком достаточности, способствуют раскрытию различных аспектов заявленной темы. Автор статьи показывает различные точки зрения по данной теме и в дальнейшем приводит собственную позицию по исследуемой проблематике.

При рассмотрении проблемы киберпреступлений необходимо сказать, что киберпреступность берёт своё начало с прошлого столетия. Как отмечают О. П. Грибунов и А. А. Баранов, с каждым появлением новых систем разрабатывались программы, способные взломать и получать данные с различных устройств. В дальнейшем компьютерные преступления начали проявляться в форме повреждения компьютерных систем: приход в информационную среду такого понятия, как «пиратство», и создание неофициальных программных продуктов, что за собой повлекло возможность несанкционированного доступа к компьютерным данным. Вследствие этого стало очевидным принятие разного рода официальных документов. Так, например, в ноябре 2001 г. в городе Будапеште (Венгрия) Советом Европы была подписана Конвенция о преступности в сфере компьютерной информации ETS № 185 [5], в которой отражались общие принципы международного сотрудничества и основные направления, направленные на защиту общества от преступности в сфере компьютерной информации [6, с. 56]. Приведенные данные являются подтверждением того, что киберпреступность постоянно развивается в вариативности своего совершения и, к сожалению, это происходит с появлением новых компьютерных инноваций.

Изучая современное состояние преступлений в IT-сфере, отметим, что за последнее десятилетие зафиксирован скачок так называемых киберпреступлений, противодействие которым в современных реалиях выходит на приоритетное направление. Как указывает представитель криминалистического центра Следственного комитета Т. Ю. Салихов, с 2014 по 2022 г. был зафиксирован практически пятидесятикратный рост IT-преступлений (10 тыс. против 510 тыс.). Также, по словам вышепоименованного, злоумышленники используют искусственный интеллект для создания фишинговых сайтов или генерации текста, который в исходном варианте выглядит как материал определенной организации [7].

Продолжая приводить статистические показатели, отметим, что в марте текущего года президент Российской Федерации В. В. Путин на расширенном заседании Министерства внутренних дел Российской Федерации (далее — МВД России) сообщил, что показатель киберпреступности составил четверть от общего числа преступного соотношения. По словам главы российского государства, борьба с данным видом преступления — одна из приоритетных задач деятельности МВД России.

Стоит добавить, что руководитель отдела по расследованию преступлений в сфере ИТТ центрального аппарата Следственного комитета России К. П. Комарда заявил, что уровень данной категории преступлений за последние семь лет вырос в 20 раз, отметив также, что сотрудники правоохранительных органов должны учитывать всю специфичность данных преступлений, взаимодействовать со специалистами в данной сфере [8].

Так, для проведения исследования средств компьютерной техники и информации необходимо привлекать грамотных специалистов, знания которых могут помочь, например, найти способы дешифрования информации, скрытой на электронных

носителях. Важной формой применения специальных знаний выступает участие в следственных действиях, например, при задержании подозреваемого лица с поличным можно проводить осмотр с работающей техникой. Данные, изъятые на электронный носитель информации, подвергаются непосредственному исследованию специалистом [9, с. 885; 10, с. 13; 11, с. 67; 12, с. 216]. Исходя из этого следует отметить, что изъятие, исследование и фиксация компьютерной информации требуют привлечения грамотных специалистов, поскольку изъятые сведения могут являться источником доказательственной базы.

Высокие технологии в современных реалиях являются неотъемлемой частью жизнедеятельности общества. С учетом всей специфики преступлений в сфере ИТТ сотрудникам полиции важно «быть на шаг впереди» киберпреступников, улучшать свои способности и знания в раскрытии и расследовании данной категории преступлений. Как было отмечено, киберпреступность растёт с каждым годом, и это является острой проблемой для сотрудников российской полиции. [13, с. 79].

Так, при рассмотрении вопроса о противодействии данной категории преступности необходимо сказать о важности подготовки и технической оснащенности сотрудников органов внутренних дел. Необходимо подчеркнуть, что за последние несколько лет государство принимает меры для интенсификации борьбы с киберпреступностью. Так, в 2020 г. в структуре МВД России начали формироваться подразделения по борьбе с киберпреступлениями. Министр внутренних дел Российской Федерации, генерал полиции В. А. Колокольцев заявил, что, «учитывая масштабы распространения киберпреступлений, разнообразие схем и методов их совершения, отсутствие единого алгоритма раскрытия, добиться кардинального улучшения невозможно, так как новые подразделения необходимо обеспечивать не только кадрами, но и современными технологиями» [14].

В связи с тем, что появляются новые способы совершения киберпреступлений, сотрудники полиции должны вырабатывать новые методы борьбы с ними, т. к. старые становятся неэффективными. Вследствие этого необходимо работать по принципу талиона, т. е. бороться с киберпреступлениями абсолютно «зеркально» — с использованием информационных технологий.

Так, не стоит на месте развитие искусственного интеллекта, который, помимо своего применения в жизнедеятельности человека (например, чат-бот ChatGPT, в последнее время широко обсуждаемый обществом), может помочь и в противодействии преступности. Следует понимать, что искусственный интеллект — это нейросеть, способная работать и выполнять подобные человеку действия в соответствии с заданным ему алгоритмом. Ни для кого не секрет, что у сотрудников полиции довольно много работы не только в плане составления процессуальных документов, но и в проведении отдельных действий (например, оперативно-розыскные мероприятия или следственные действия). Вследствие сказанного искусственный интеллект может помочь сотрудникам правоохранительных органов в их деятельности, и в частности в борьбе с киберпреступлениями. Преимущество искусственного интеллекта — умение выбирать нужную информацию из исходного большого массива сведений.

Например, полицейские лондонского Нью-Скотланд-Ярда используют искусственный интеллект в расследованиях преступлений, где за небольшой промежуток времени необходимо обработать большие массивы данных. Раньше на их изучение команда могла затратить целые месяцы, а сейчас, без преувеличения, — считаные часы. Степень

напряжения довольно высока, т. к. полицейские должны найти необходимые улики за ограниченное время, которое отводится на содержание подозреваемого под стражей. В ходе одного из расследований команде сотрудников Нью-Скотланд-Ярда потребовалось просмотреть около 70 тыс. сообщений в мессенджере. На это могло быть затрачено три месяца постоянной работы лаборатории из 150 человек. А если учесть, что следователи работают одновременно над несколькими делами, то время поисков могло бы увеличиться в разы [15].

Рассмотрим, как информационные технологии применяются для противодействия киберпреступности на зарубежном опыте. Так, в уголовном процессе США весьма активно идет применение самых новейших разработок, которые позволяют оптимизировать процессуальные действия, приводящие к успешному расследованию преступлений в исследуемой автором статьи сфере. Например, активно применяется система распознавания лиц, которая, несомненно, практична и удобна с точки зрения идентификации человека и сокращения времени для правоохранительных органов.

В Великобритании используются геномные базы данных, основанные на STR-I полиморфизме ДНК (STR — Short Tandem Repeats). Технические возможности помогают идентифицировать человека по его биологическим материалам [16, с.162].

В Канаде активно применяется подача и онлайн-регистрация процессуальных документов, а при помощи веб-интерфейса участники судопроизводства могут детально ознакомиться с материалами уголовного дела [17, с.25].

Необходимо подчеркнуть, что является важным развивать и применять новые технологии в расследовании преступлений, что эффективно скажется как на противодействии им, так и в перспективе на их предотвращении (профилактике). Полагаем нужным упомянуть и о том, что применение данных технологий сократит время на проведение оперативно-розыскных и следственных мероприятий, что позволит осуществлять иные процессуальные действия. В частности, при работе с большим объёмом информации целесообразно применять искусственный интеллект, который на определенной алгоритмизации выполняет так называемую выборку, т. е. осуществляет поиск нужных сведений. Например, если следователю необходимо проанализировать большой объём информации (прочитать на изъятом компьютере подозреваемого лица около 100 тыс. сообщений и найти сведения преступного характера), то на это будет затрачен солидный запас времени. В этом случае искусственный интеллект может стать существенным подспорьем для следователя в поиске нужной информации. Лица, совершающие IT-преступления, могут иметь соучастников, поэтому анализ всех сообщений может дать нужную информацию для расследования уголовного дела.

Ведя речь об искусственном интеллекте, отметим, что он может применяться также для распознавания лица — на основе его биометрических данных; анализа голоса — его тон, наличие дефектов и т. п. (особенно актуально для онлайн-мошенников, когда, например, оперативные сотрудники могут получать результаты оперативно-розыскного мероприятия «Прослушивание телефонных переговоров» и с помощью искусственного интеллекта анализировать его соответствие с задержанным преступником); построения следственных версий и, соответственно, следственных действий по ним; анализа поведения человека (например, при допросе). Отметим, что искусственный интеллект может также использоваться в качестве переводчика при допросе для лица, не владеющего государственным языком.

Специфика расследования киберпреступлений заключается в том, при проведении

отдельных следственных или процессуальных действий необходимо получение судебного решения. Так, например, в соответствии со ст. 186.1 Уголовно-процессуального кодекса Российской Федерации, следователь получает разрешение у суда на получение информации о сотовой связи. В данной связи необходимо сказать о мобильности киберпреступников, т. е. их возможности совершать противоправные действия в одном месте и непосредственно после их реализации менять своё местонахождение. Применительно к этому можно заметить, что преступник имеет возможность скрыться от сотрудников правоохранительных органов и тем самым уйти от ответственности. В этом случае будет целесообразно рассмотреть вопрос о более быстром получении судебного решения, что в целом эффективно скажется на расследовании киберпреступлений [18, с. 78—79].

Считаем резонным остановиться и на категории «пользователь» интернет-пространства. Таковым может быть любое лицо, имеющее соответствующий выход в информационно-телекоммуникационную сеть Интернет. Злоумышленнику будет выгодно, если «новенький» пользователь, т. е. непродолжительное время пользующийся гаджетом или сам по себе доверчивый, тем самым легко поддаётся на манипуляции. Жертвами киберпреступников могут становиться лица любого возраста. Это может быть подросток, недавно начавший использовать смартфон, или пожилой человек, который, получив «интересное предложение» от злоумышленника, может поддаться на его преступные манипуляции. Здесь уместно также вспомнить о то же банковском мошенничестве, когда злоумышленник звонит и представляется сотрудником банка, после чего пытается осуществить мошеннические действия.

Неоспоримой, как видится автору, является точка зрения С. В. Пархоменко и К. Н. Евдокимовой о том, что «профилактика компьютерных преступлений является одним из главных направлений деятельности правоохранительных органов по обеспечению информационной безопасности российского общества» [19, с. 266]. Вследствие этого работает правило «предупреждён — значит вооружён».

С учетом вышеизложенного однозначно важно проводить профилактические мероприятия, причём инициаторами таковых могут быть не только сотрудники полиции, но и представители сотовых компаний или кибердружинники (лица, оказывающие содействие сотрудникам правоохранительных органов). Несомненно, с развитием информационных технологий киберпреступники способны продумывать новые методы совершения противоправных действий, но с точки зрения их профилактики преждевременная осведомленность населения будет являться важным ключом для противодействия данной категории преступлений.

Таким образом, на основе анализа современного состояния кибепреступности можно утверждать, что необходимо совершенствовать методы её противодействию, принимая во внимание научно-технический прогресс, параллельно которому злоумышленники постоянно вырабатывают новые преступные схемы. Как было отмечено, следует «быть на шаг впереди» киберпреступников, и в приоритете это достижимо путем развития необходимых знаний и навыков у сотрудников правоохранительных органов по противодействию преступлениям, совершенным с использованием IT-технологий. Принимая во внимание динамичное развитие и использование информационных технологий во многих сферах жизнедеятельности, считаем, что их применение в деятельности сотрудников полиции весьма целесообразно, как, например, использование искусственного интеллекта полицейских лондонского Нью-Скотланд-Ярда. Также с целью профилактики видится рациональным повышать осведомленность

населения по безопасному использованию цифровых технологий, уведомляя о «типичных» махинациях киберпреступников.

Возникновение новых компьютерных программ, способов, методов и средств в сфере выявления и расследования преступлений имеет большое практическое значение для более успешного противодействия преступлениям в сфере информационных технологий. Теперь сотрудники правоохранительных органов могут более оперативно выявлять следы преступлений, моделировать образы преступников, собирать доказательства и др. В перспективе внедрение новых информационных технологий поможет снизить количество совершения IT-преступлений, а также повысить процент их раскрываемости. Так, автором статьи сообщено о практической возможности применения искусственного интеллекта в раскрытии и расследовании IT-преступлений.

В век информационных технологий происходит и совершенствование способов и видов совершения преступлений, и в частности в сфере информационных технологий, поэтому одна из главных задач успешной деятельности правоохранительных органов в части выявления и расследования преступлений является необходимость внедрения и успешного использования IT-технологий в борьбе с преступными деяниями.

Таким образом, безусловно, необходимо дальнейшее создание и внедрение информационных технологий в повседневную деятельность правоохранительных органов Российской Федерации.

Библиография

1. Косырев А. С. Киберпреступность: правовой аспект / А. С. Косырев, А. В. Лошкарев // MODERN SCIENCE. – 2019. – № 5 (1). – С. 221-227. DOI: 10.22394/2686-7834-2022-1-83-88.
2. Андриенко Ю. А. Отдельные аспекты использования информационных технологий и работы с электронными носителями информации в доказывании по уголовным делам // Вестник Сибирского юридического института МВД России. – 2018. – № 3 (32). – С. 99-105 [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/otdelnye-aspekty-ispolzovaniya-informatsionnyh-tehnologiy-i-raboty-s-elektronnymi-nositelyami-informatsii-v-dokazyvanii-po-ugolovnym (дата обращения: 02.09.2023).
3. Тимофеев С. В. Выявление и предупреждение преступлений в сети Интернет: проблемы и пути их решения / С. В. Тимофеев, Э. Ю. Пороховой // Вестник Восточно-Сибирского института МВД России. – 2021. – № 4. – С. 220-229. DOI: 10.24412/2312-3184-2021-4-220-229.
4. Вестник студенческого научного общества ГОУ ВПО «ДОННУ». – Донецк: ДОННУ, 2022. – Вып. 14. – Т. 4: Юриспруденция. Ч. 2. – 247 с.
5. Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 нояб. 2001 г.).
6. Грибунов О. П. Некоторые аспекты противодействия IT-преступлениям / О. П. Грибунов, А. А. Баранов // Деятельность правоохранительных органов в современных условиях. – 2020. – С. 55-61. DOI: 10.55001/2587-9820.2022.82.45.014.
7. Число киберпреступлений в России. 2023 // TADVISER. Государство. Бизнес. Технологии: портал выбора технологий и поставщиков [Электронный ресурс]. – URL: https://www.tadviser.ru/index.php/ (дата обращения: 06.09.2023).
8. Фурсеев И. Путин словами «мы не успеваем» объяснил рост числа преступлений в ИТ. 2021 // RBC.RU. Последние новости дня в России и мире сегодня Электронный

ресурс] – URL: https://www.rbc.ru/politics/03/03/2021/603f6ae59a7947b29b0e9b18 (дата обращения: 08.09.2022).

9. Лантух Э. В. Использование специальных знаний при расследовании преступлений в сфере компьютерной информации / Э. В. Лантух, В. С. Ишигеев, О. П. Грибунов // Всероссийский криминологический журнал. – 2020. – № 6. – С. 882—890 [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/ispolzovanie-spetsialnyh-znaniy-pri-rassledovanii-prestupleniy-v-sfere-kompyuternoy-informatsii (дата обращения: 03.09.2023). DOI 10.17150/2500-4255.2020.14(6).882-890.
10. Балашова А. А. Электронные носители информации и их использование в уголовно-процессуальном доказывании: автореф. дис. ... канд. юрид. наук / А. А. Балашова. – М., 2020. – 31 с.
11. Проблемы борьбы с преступностью в условиях цифровизации: сб. ст. XIX междунар. науч.-практ. конф. «Уголовно-процессуальные и криминалистические чтения на Алтае», посв. памяти Вениамина Константиновича Гавло. — Вып. XVII / отв. ред. С. И. Давыдов, В. В. Поляков. – Барнаул: Изд-во Алт. ун-та, 2021. – 500 с.
12. Третьякова Е. И. Значение цифровой информации в расследовании преступлений / Е. И. Третьякова, Ю. Л. Соловьёва, Н. А. Полторацкий, А. А. Остапенко // Научный дайджест Восточно-Сибирского института МВД России – 2020. – № 6 (9). – С. 214-219.
13. Малыхина Т. А. Некоторые особенности современных тенденций преступности в России // Деятельность правоохранительных органов в современных условиях. – 2021. – С. 79-83.
14. Число IT-преступлений в России выросло с начала года на 75,2 % // РИА Новости [Электронный ресурс]. — URL: https://ria.ru/20200228/1565305566.html (дата обращения: 07.09.2023).
15. Вас охраняет нейросеть: как искусственный интеллект помогает искать преступников // RBC.RU. Последние новости дня в России и мире сегодня [Электронный ресурс] – URL: https://fisher.rbc.ru/article.html?utm_source=rbc&utm_medium=main&utm_campaign=more23w-a-df-m&from=column_15 (дата обращения: 09.09.2023).
16. Современные направления развития криминалистических методик и технологий в уголовном судопроизводстве: моногр. / под науч. ред. Д. В. Кима; отв. ред. А. И. Баянов. – Красноярск: Сиб. федер. ун-т, 2020. – 244 с. ISBN 978-5-7638-4273-9.
17. Информационные технологии в уголовном процессе зарубежных стран: моногр. / Колл. авт.; под ред. С. В. Зуева. – М., 2020 – С. 216.
18. Алиев Т. Ф. Киберпреступность: современное состояние и актуальные проблемы / Т. Ф. Алиев, С. И. Усачев // Искусство правоведения. The art of law. – 2023. – № 1 (5). – С. 92.
19. Пархоменко С. В. Предупреждение компьютерной преступности в Российской Федерации: интегративный и комплексный подходы / С. В. Пархоменко, К. Н. Евдокимов // Всероссийский криминологический журнал. – 2015. – № 2. – С. 265—276 [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/preduprezhdenie-kompyuternoy-pr (дата обращения: 12.09.2023). DOI: 10.17150/1996-7756.2015.9(2).265-276

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.

Со списком рецензентов издательства можно ознакомиться здесь.

РЕЦЕНЗИЯ
на статью на тему «Вопросы противодействия преступлениям, совершаемым с использованием IT-технологий».

Предмет исследования.
Предложенная на рецензирование статья посвящена актуальным вопросам противодействия преступлениям, совершаемым с использованием IT-технологий. Автором рассматривается актуальной заявленной тематики, зарубежный опыт, а также некоторые практические аспекты темы. В качестве предмета исследования выступили эмпирические данные, нормы российского права, зарубежный опыт.

Методология исследования.
Цель исследования прямо в статье не заявлена. При этом она может быть ясно понята из названия и содержания работы. Цель может быть обозначена в качестве рассмотрения и разрешения отдельных проблемных аспектов вопроса о противодействия преступлениям, совершаемым с использованием IT-технологий. Исходя из поставленных цели и задач, автором выбрана методологическая основа исследования.
В частности, автором используется совокупность общенаучных методов познания: анализ, синтез, аналогия, дедукция, индукция, другие. В частности, методы анализа и синтеза позволили обобщить и разделить выводы различных научных подходов к предложенной тематике, а также сделать конкретные выводы из эмпирический данных.
В частности, следует положительно оценить возможности эмпирического метода исследования, благодаря которому, в частности, удалось уточнить актуальность и значимость тематики. В частности, отметим следующий авторский вывод по исследованию: «Изучая современное состояние преступлений в IT-сфере, отметим, что за последнее десятилетие зафиксирован скачок так называемых киберпреступлений, противодействие которых в современных реалиях выходит на приоритетное направление. Как указывает представитель криминалистического центра Следственного комитета Темирлан Салихов, с 2014 по 2022 год был зафиксирован практически 50-кратный рост IT-преступлений (10 тысяч против 510 тысяч киберпреступлений). Также по словам представителя, злоумышленники используют искусственный интеллект для создания фишинговых сайтов или генерации текста, который в исходном варианте выглядит как материал определенной организации или фракции [7]. Продолжая приводить статистические показатели, отметим, что в марте текущего года президент Российской Федерации (далее по тексту – РФ) В.В. Путин на расширенном заседании Министерства внутренних дел РФ (далее по тексту – МВД РФ) сообщил, что показатель киберпреступности составил четверть от общего числа преступного соотношения. По словам главы государства, борьба с данным видом преступления – одна из приоритетных задач деятельности МВД РФ».
Также автор использует опыт зарубежных стран по заявленным в статье проблемам. Например, отмечается следующее: «В Великобритании при расследовании преступлений в сфере информационных технологий применяют электронные устройства для обнаружения следов преступления и производства следственных действий. В силу применения данных электронных устройств фиксируется доказательственная база, которая в дальнейшем используются в суде. В Канаде активно применяется подача и регистрация онлайн процессуальных документов, а при помощи Веб-интерфейса участники судопроизводства могут детально ознакомиться с материалами уголовного дела»».

Таким образом, выбранная автором методология в полной мере адекватна цели исследования, позволяет изучить все аспекты темы в ее совокупности.

Актуальность.

Актуальность заявленной проблематики не вызывает сомнений. Имеется как теоретический, так и практический аспекты значимости предложенной темы. С точки зрения теории тема противодействия преступлениям, совершаемым с использованием IT-технологий сложна и неоднозначна. Действительно, в современном мире технологии используются не только законопослушными субъектами. В связи с этим встает вопрос об обеспечении национальной кибербезопасности. Сложно спорить с автором статьи в том, что «Развитие информационных технологий, в частности, сказалось на новых способах совершения киберпреступлений. Так, компьютерная сеть превратилась в новый эффективный инструмент бизнеса и новый мощный канал распространения преступных деяний. В связи с этим необходимо прорабатывать наиболее оптимальные и эффективные формы их противодействия».

Тем самым, научные изыскания в предложенной области стоит только поприветствовать.

Научная новизна.

Научная новизна предложенной статьи требует уточнений. Во-первых, она может быть выражена в конкретных выводах автора. Среди них, например, такой вывод:

«проанализировав современное состояние кибепреступности, необходимо совершенствовать методы её противодействия, принимая во внимание научно-технический прогресс, параллельно которому злоумышленники постоянно вырабатывают новые преступные схемы. Как было отмечено, необходимо «быть на шаг впереди» киберпреступников, и в приоритете это достижимо путем развития необходимых знаний и навыков у сотрудников правоохранительных органов по противодействию преступлениям, совершенным с использованием IT-технологий. Принимая во внимание динамичное развитие и использование информационных технологий во многих сферах жизнедеятельности, целесообразно их применение в деятельности сотрудников полиции, как, например, использование искусственного интеллекта полицейских лондонского Скотланд-Ярда. Также с целью профилактики рационально проводить осведомленность населения по безопасному использованию цифровых технологий, уведомляя о «типичных» преступных махинациях киберпреступников».

При этом указанный вывод не обладает научной новизной представляет собой выводы иных авторов или обобщение опыта зарубежных юрисдикций. В связи с этим стоит уточнить авторскую позицию на наличие в ней научной новизны.

Во-вторых, автором предложены некоторые обобщения, например, зарубежной практики, но не всегда дается авторский оригинальный комментарий к ним. В частности, можно было бы сопоставить российский и зарубежный опыт, выявить те или иные тенденции и пр.

Таким образом, материалы статьи могут иметь определенных интерес для научного сообщества с точки зрения развития вклада в развитие науки, но только после уточнения именно авторского вклада, научной новизны по статье.

Стиль, структура, содержание.

Тематика статьи соответствует специализации журнала «Юридические исследования», так как она посвящена правовым проблемам, связанным с расследованием преступлений.

Содержание статьи в полной мере соответствует названию, так как автор рассмотрел заявленные проблемы, в целом достиг цели исследования.

Качество представления исследования и его результатов следует признать в полной мере положительным. Из текста статьи прямо следуют предмет, задачи, методология и основные результаты исследования.
Оформление работы в целом соответствует требованиям, предъявляемым к подобного рода работам. Существенных нарушений данных требований не обнаружено.

Библиография.
Следует высоко оценить качество использованной литературы. Автором активно использована литература, представленная авторами из России (Алиев Т.Ф., Усачев С.И., Пархоменко С.В., Евдокимов К.Н., Третьякова Е.И., Соловьёва Ю.Л., Полторацкий Н.А. Остапенко А.А. и другие). Многие из цитируемых ученых являются признанными учеными в области расследования киберпреступлений.
Таким образом, труды приведенных авторов соответствуют теме исследования, обладают признаком достаточности, способствуют раскрытию различных аспектов темы.

Апелляция к оппонентам.
Автор провел серьезный анализ текущего состояния исследуемой проблемы. Все цитаты ученых сопровождаются авторскими комментариями. То есть автор показывает разные точки зрения на проблему и пытается аргументировать более правильную по его мнению.

Выводы, интерес читательской аудитории.
Выводы в полной мере являются логичными, так как они получены с использованием общепризнанной методологии. Статья может быть интересна читательской аудитории в плане наличия в ней систематизированных позиций автора применительно к вопросам противодействия преступлениям, совершаемым с использованием IT-технологий, но только после уточнения научной новизны приведенной статьи.

На основании изложенного, суммируя все положительные и отрицательные стороны статьи
«Рекомендую отправить на доработку»

Результаты процедуры повторного рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Предметом исследования в представленной на рецензирование статье являются, как это следует из ее наименования, вопросы противодействия преступлениям, совершаемым с использованием IT-технологий. Заявленные границы исследования соблюдены автором.
Методология исследования в тексте статьи не раскрывается, но очевидно, что ученым использовались всеобщий диалектический, логический, статистический, сравнительно-правовой, формально-юридический методы исследования.
Актуальность избранной автором темы исследования обоснована следующим образом: "... прогресс IT-технологий помимо своих неоспоримых преимуществ имеет и обратную сторону медали: всё более распространенным является совершение мошенничеств, вымогательств, хакерских взломов, незаконного оборота наркотических средств, распространения вирусных программ и проявления других противоправных действий с использованием информационных технологий [1, с. 221-224]. Всем известен факт: «состояние преступности является своеобразным отражением, индикатором процессов,

происходящих в обществе» [2, с. 99]. Развитие информационных технологий, в частности, сказалось на новых способах совершения киберпреступлений. Так, компьютерная сеть превратилась в новый эффективный инструмент бизнеса и новый мощный канал распространения преступных деяний. В связи с этим необходимо прорабатывать наиболее оптимальные и эффективные формы их противодействия [3, с. 222; 4, с. 16]". Дополнительно ученому необходимо перечислить фамилии ведущих специалистов, занимавшихся исследованием поднимаемых в статье проблем, а также раскрыть степень их изученности.

Научная новизна работы проявляется в ряде предложений автора: "... важно проводить профилактические мероприятия, при чём их инициаторами могут быть не только сотрудники полиции, но и представители сотовых компаний или кибердружинники (лица, оказывающие содействие сотрудникам правоохранительных органов). Несомненно, с развитием информационных технологий киберпреступники могут продумывать новые методы совершения противоправных действий, но с точки зрения их профилактики преждевременная осведомленность населения будет являться важным ключом для противодействия данной категории преступности"; "Принимая во внимание динамичное развитие и использование информационных технологий во многих сферах жизнедеятельности, целесообразно их применение в деятельности сотрудников полиции, как, например, использование искусственного интеллекта..."; "... совершенствования путем появления новых компьютерных программ, способов, методов и средств в сфере выявления и расследования преступлений имеет важное практическое значение для более успешного противодействия преступлениям в сфере информационных технологий. Теперь сотрудники правоохранительных органов могут более оперативно выявлять следы преступлений, моделировать образы преступников, собирать доказательства и др. В перспективе, внедрение новых информационных технологий поможет снизить количество совершения IT-преступлений, а также повысить процент их раскрываемости" и др. Таким образом, статья вносит определенный вклад в развитие отечественной правовой науки и заслуживает внимания читательской аудитории, но некоторые ее положения нуждаются в уточнении и конкретизации.

Научный стиль исследования выдержан автором в полной мере.

Структура работы вполне логична. Во вводной части статьи автор обосновывает актуальность избранной им темы исследования. В основной части статьи ученый рассматривает ряд мер по противодействию преступлениям, совершаемым с использованием IT-технологий, анализирует соответствующий положительный зарубежный опыт, дает рекомендации по совершенствованию мер борьбы с исследуемой категорией преступлений. В заключительной части статьи содержатся выводы по результатам проведенного исследования.

Содержание статьи соответствует ее наименованию, но не лишено некоторых недостатков.

Так, автор пишет: "Рассмотрим, как информационные технологии применяются при противодействии киберпреступности на зарубежном опыте. «Так, уголовный процесс США - очень активно идет применение самых новейших разработок, которые позволяют оптимизировать процессуальные действия, приводящие к успешному расследованию преступлений, в исследуемой нами сфере". О каких конкретно разработках в США идет речь, автор не говорит. Очевидно, что часть текста пропущена.

Ученый отмечает: "В Великобритании при расследовании преступлений в сфере информационных технологий применяют электронные устройства для обнаружения следов преступления и производства следственных действий". О каких именно электронных устройствах идет речь?

Библиография исследования представлена 18 источниками (международным

документом, монографией, научными статьями, аналитическими и статистическими данными). С формальной точки зрения этого достаточно; с фактической - некоторые положения статьи нуждаются в уточнении.

Апелляция к оппонентам как таковая отсутствует, что недопустимо для научной статьи. Автор ссылается на ряд теоретических работ исключительно для подтверждения своих суждений либо для иллюстрирования отдельных положений статьи.

Выводы по результатам проведенного исследования имеются ("... является важным развивать и применять новые технологии в расследовании преступлений, что эффективно как на их противодействии, так и в перспективе на их предотвращении (профилактике). Необходимо также сказать о том, что их применение сократит время на проведение оперативно-розыскных и следственных мероприятий, что позволит осуществлять иные процессуальные действия. В частности, при работе с большим объёмом информации, целесообразно применять искусственный интеллект, который на определенной алгоритмизации выполняет так называемую «выборку», то есть осуществляет поиск нужных сведений. Например, если следователю необходимо проанализировать большой объём информации: прочитать на изъятом компьютере подозреваемого лица около 100 тысяч сообщений и найти сведения преступного характера, то на это уйдет очень много времени. В этом случае искусственный интеллект может стать верным помощником следователя для поиска нужной информации. Лица, совершающие IT-преступления, могут иметь соучастников, поэтому анализ всех сообщений может дать нужную информацию для расследования уголовного дела. Рассматривая искусственный интеллект, отметим, что он может применяться также для распознавания лица – на основе его биометрических данных; анализа голоса – его тон, наличие дефектов и т.п. (особенно актуально для онлайн мошенников, когда, например, оперативные сотрудники могут получать результаты оперативно-розыскного мероприятия «Прослушивание телефонных переговоров» и с помощью искусственного интеллекта анализировать его соответствие с задержанным преступником); построения следственных версий и соответственно следственных действий к ним; анализа поведения человека (например, при допросе). Отметим, что искусственный интеллект может также использоваться в качестве переводчика при допросе для лица, который не владеет русским языком. В век информационных технологий происходит и совершенствование способов и видов совершения преступлений, и в частности в сфере информационных технологий, поэтому одна из главных задач успешной деятельности правоохранительной органов в части выявления и расследования преступлений, является необходимость внедрения и успешного использования IT-технологий в борьбе с преступными деяниями. Таким образом, дальнейшее создание и внедрение информационных технологий в работу правоохранительных органов"), однако нуждаются в доработке. Выводы должны быть краткими, четкими и конкретными. Примеры, иллюстрирующие отдельные положения работы, необходимо приводить в основной части статьи. Статья не должна содержать заключения, которые не подвергались детальному обсуждению в основной части исследования. Наконец, в последнем предложении пропущена часть текста.

Статья нуждается в дополнительном вычитывании с привлечением специалиста-филолога. В ней встречаются опечатки, орфографические, пунктуационные, синтаксические, стилистические ошибки, что затемняет смысл текста и затрудняет его чтение.

Интерес читательской аудитории к представленной на рецензирование статье может быть проявлен прежде всего со стороны специалистов в сфере уголовного права и криминологии при условии ее доработки: раскрытии методологии исследования, дополнительном обосновании актуальности его темы, введении дополнительных

элементов дискуссионности, уточнении отдельных положений работы, формулировании четких и конкретных выводов по результатам проведенного исследования, устранении нарушений в оформлении работы.

Результаты процедуры окончательного рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Предмет исследования. В рецензируемой статье "Вопросы противодействия преступлениям, совершаемым с использованием IT-технологий" предметом исследования являются существующие способы и приемы борьбы с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий (IT-технологий), в том числе в сравнительно-правовом аспекте.
Методология исследования. По содержанию статьи можно заключить, что автором использовались многие современные методы исследования, как общенаучные, так и частные. Методологический аппарат работы составили следующие диалектические приемы и способы научного познания: анализ, абстрагирование, индукция, дедукция, гипотеза, аналогия, синтез, типология, классификация, систематизация и обобщение. Применялись автором такие методы, как: исторический, теоретико-прогностический, формально-юридический, системно-структурный, правового моделирования, сравнительного правоведения и др. Применение современных научных методов (приемов и способов) позволило изучить сложившиеся подходы, взгляды на проблему, выработать авторскую позицию и аргументировать ее. Также, можно отметить, что в статье использовалось сочетание теоретической и эмпирической информации.
Актуальность исследования. Актуальность данной темы не вызывает сомнения. Цифровизация всех сфер жизнедеятельности не только создает определенные удобства, но и обеспечивает большие возможности для совершения противоправных действий с использованием информационно-коммуникационных технологий, т.н. киберпреступлений. Киберпреступность - это сравнительно новое социальное явление (как общественно опасное деяние), и соответственно, не все вопросы противодействия ей разрешены на уровне законодательства и правоприменения. По этой причине любые научные разработки по данной проблеме заслуживают внимания и могут иметь практическую значимость.
Научная новизна. Нельзя сказать, что автор этой статьи впервые в отечественной юриспруденции обратился к вопросам противодействия преступлениям, совершаемым с использованием IT-технологий. Однако, проведенное им исследование имеет элементы научной новизны, некоторые выводы и предложения заслуживают внимания (например, "Принимая во внимание динамичное развитие и использование информационных технологий во многих сферах жизнедеятельности, считаем, что их применение в деятельности сотрудников полиции весьма целесообразно, как, например, использование искусственного интеллекта... Также с целью профилактики видится рациональным повышать осведомленность населения по безопасному использованию цифровых технологий, уведомляя о «типичных» махинациях киберпреступников").
Стиль, структура, содержание. В целом статья написана научным стилем, используется специальная научная терминология. Материал изложен последовательно и грамотно. Однако работа не лишена недостатков, например, вызывает сомнение корректность словосочетания "цифровизация населения" или присутствуют некоторые стилистические ошибки (например, повторы слов в предложении (...использование...использование) и др.). Однако отмеченные замечания являются устранимыми и не умаляют проделанной

автором работы. Статья логически структурирована. По содержанию статья соответствует своему названию. Тема раскрыта. В качестве пожелания автору можно указать на необходимость доработки вводной и заключительной части статьи, поскольку в научных публикациях к ним предъявляются специальные требования.

Библиография. Автором использовано достаточное количество доктринальных источников. Ссылки на библиографические источники оформлены правильно.

Апелляция к оппонентам. В работе присутствует научная полемика. Все обращения к оппонентам корректные.

Выводы, интерес читательской аудитории. Статья "Вопросы противодействия преступлениям, совершаемым с использованием IT-технологий" рекомендуется к опубликованию, т.к. отвечает требованиям, предъявляемым к научным публикациям, написана на актуальную тему, отличается научной новизной и может иметь практическую значимость. Данная статья может представлять интерес для широкой читательской аудитории, прежде всего, для специалистов в области уголовно-процессуального права и криминалистики, а также для преподавателей и обучающихся юридических вузов и факультетов.